

DEVICE AND METHOD FOR CIPHERING, DEVICE AND METHOD FOR DECIPHERING, CIPHER SYSTEM AND RECORDING MEDIUM WHICH STORES THE PROGRAM

Publication number: JP2001222218

Publication date: 2001-08-17

Inventor: OKAMOTO TATSUAKI; DAVID POANSHEBARU

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- International: G09C1/00; G09C1/00; (IPC1-7): G09C1/00

- European:

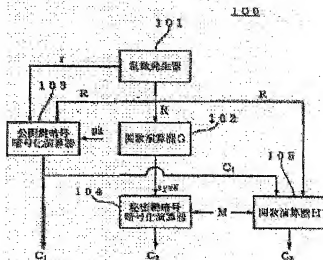
Application number: JP20000032461 20000209

Priority number(s): JP20000032461 20000209

Report a data error here

Abstract of JP2001222218

PROBLEM TO BE SOLVED: To obtain a high degree of safety against an active attack with respect to a ciphered sentence by a public key ciphering. **SOLUTION:** In a ciphering device 100, M is a plain sentence having (t) bits and a random number generator 101 generates a (k) bit random number R and a one bit random number (r). A function computer G102 computes a secret key $\text{sym}K = G(R)$ by using the number R. Moreover, a ciphered sentence $C1 = \text{Epk}(R, r)$ is generated by a public key cipher ciphering computer 103 by using the numbers R and (r) and a public key pk. Furthermore, by using the key $\text{sym}K$ and the sentence M, a ciphered sentence $C2 = \text{symEsymk}(M)$ is generated by a secret key cipher ciphering computer 104. Then, a function computer H105 computes $C3 = H(C1, R, M)$ and $C = (C1, C2, C3)$ is outputted as a ciphered sentence.



Data supplied from the esp@cenet database - Worldwide

(18) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-222218

(P2001-222218A)

(43) 公開日 平成13年8月17日 (2001.8.17)

(51) Int. Cl.⁷

G 0 9 C 1 / 0 0

識別番号

6 2 0

F I

C 0 9 C 1 / 0 0

データベース (参考)

6 2 0 Z 5 J 1 0 4

審査請求 未請求 請求項の数13 O L (全 6 頁)

(21) 出願番号 特願2000-32461 (P2000-32461)

(22) 出願日 平成12年2月9日 (2000.2.9)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 岡本 領明

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社内

(73) 発明者 ダビド ポアンシェバル

フランス・75230・パリ・セドゥ・05・

ル・ダルム・45

(74) 代理人 100064908

弁理士 志賀 正武

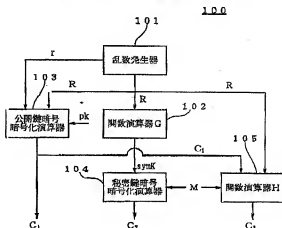
Fデータベース (参考) 5J104 JA21 JA30 JA31 NA02

(54) 【発明の名称】 暗号化装置、方法、復号装置、方法、暗号システム及びプログラムを記憶した記憶媒体

(57) 【要約】

【課題】 公開鍵暗号による暗号文に対する能動的な攻撃に対して高い安全性が得られるようにする。

【解決手段】 暗号化装置100において、 t ビットの平文を M とし、乱数発生器101より k ビットの乱数 R 及び1ビットの乱数 r を発生させる。関数演算器G102により R を用いて秘密鍵 $symK = G(R)$ を計算する。また、公開鍵暗号暗号化演算器103により、 R 、 r と公開鍵 pk とを用いて暗号文 $C_1 = E_{pk}(R, r)$ を生成する。また、秘密鍵暗号暗号化演算器104により、上記秘密鍵 $symK$ と平文 M とを用いて暗号文 $C_2 = symE_{symK}(M)$ を生成する。さらに、関数演算器H105により $C_3 = H(C_1, R, M)$ を計算し、 $C = (C_1, C_2, C_3)$ を暗号文として出力する。



(2) 001-222218 (P2001-222218A)

【特許請求の範囲】

【請求項1】 乱数 R 、 r を発生する乱数発生手段と、上記乱数 R 、 r と公開鍵 p 、 k とを用いて暗号文 $C_1 = E_{pk}(R, r)$ を計算する公開鍵暗号暗号化演算手段と、上記乱数 R と関数 G とを用いて秘密鍵 s 、 $ymk = G(R)$ を計算する第1の関数演算手段と、上記秘密鍵 s 、 ymk と平文 M とを用いて暗号文 $C_2 = smE_{symk}(M)$ を計算する秘密鍵暗号暗号化演算手段と、

上記乱数 R と上記暗号文 C_1 と上記平文 M と関数 H とを用いて暗号文 $C_3 = H(C_1, R, M)$ を計算する第2の関数演算手段と、

暗号文 $C = (C_1, C_2, C_3)$ を出力する出力手段とを設けたことを特徴とする暗号化装置。

【請求項2】 上記関数 H を任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数 G を k ビットのデータを s ビットに変換するランダム関数とすることを特徴とする請求項1記載の暗号化装置。

【請求項3】 乱数 R 、 r と公開鍵 p 、 k とを用いて計算された暗号文 $C_1 = E_{pk}(R, r)$ と、上記乱数 R と関数 G とを用いて計算された秘密鍵 s 、 $ymk = G(R)$ と平文 M とから計算された暗号文 $C_2 = smE_{symk}(M)$ と、上記乱数 R と上記暗号文 C_1 と関数 H とを用いて計算された暗号文 $C_3 = H(C_1, R, M)$ とからなる暗号文 $C = (C_1, C_2, C_3)$ を入力する入力手段と、

上記暗号文 C_1 と秘密鍵 s 、 k とを用いて乱数 $R' = D_{sk}(C_1)$ を計算する公開鍵暗号復号演算手段と、

上記乱数 R' と上記関数 G とを用いて秘密鍵 s 、 $ymk' = G(R')$ を計算する第1の関数演算手段と、

上記秘密鍵 s 、 ymk' と上記暗号文 C_2 とを用いて平文 $M' = smD_{symk'}(C_2)$ を計算する秘密鍵暗号復号演算手段と、

上記平文 M' と上記暗号文 C_1 と上記乱数 R' と上記関数 H とを用いて暗号文 $C_3' = H(C_1, R', M')$ を計算する第2の関数演算手段と、

上記暗号文 C_3' と上記暗号文 C_2 とを比較する比較手段とを設けたことを特徴とする復号装置。

【請求項4】 上記関数 H を任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数 G を k ビットのデータを s ビットに変換するランダム関数とすることを特徴とする請求項3記載の復号装置。

【請求項5】 乱数 R 、 r を発生する乱数発生手段と、上記乱数 R 、 r と公開鍵 p 、 k とを用いて暗号文 $C_1 = E_{pk}(R, r)$ を計算する公開鍵暗号暗号化演算手段と、上記乱数 R と関数 G とを用いて秘密鍵 s 、 $ymk = G(R)$ を計算する第1の関数演算手段と、

上記秘密鍵 s 、 ymk と平文 M とを用いて暗号文 $C_2 = s$

$ymE_{symk}(M)$ を計算する秘密鍵暗号暗号化演算手段と、

上記乱数 R と上記暗号文 C_1 と上記平文 M と上記関数 H とを用いて暗号文 $C_3 = H(C_1, R, M)$ を計算する第2の関数演算手段と、

暗号文 $C = (C_1, C_2, C_3)$ を出力する出力手段とを有する暗号化装置と、

上記暗号文 $C = (C_1, C_2, C_3)$ を入力する入力手段と、

上記暗号文 C_1 と秘密鍵 s 、 k とを用いて乱数 $R' = D_{sk}(C_1)$ を計算する公開鍵暗号復号演算手段と、

上記乱数 R' と上記関数 G とを用いて秘密鍵 s 、 $ymk' = G(R')$ を計算する第3の関数演算手段と、

上記秘密鍵 s 、 ymk' と上記暗号文 C_2 とを用いて平文 $M' = smD_{symk'}(C_2)$ を計算する秘密鍵暗号復号演算手段と、

上記平文 M' と上記暗号文 C_1 と乱数 R' と上記関数 H とを用いて暗号文 $C_3' = H(C_1, R', M')$ を計算する第4の関数演算手段と、

上記暗号文 C_3' と上記暗号文 C_2 とを比較する比較手段とを有する復号装置とを備えたことを特徴とする暗号システム。

【請求項6】 上記関数 H を任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数 G を k ビットのデータを s ビットに変換するランダム関数とすることを特徴とする請求項5記載の暗号システム。

【請求項7】 m を平文（暗号の対象となる文書）、 r を乱数、 (p, k, s, k) を公開鍵と秘密鍵の対とすると、 p, k, m, r より暗号文 $C = E_{pk}(m, r)$ が作られるような公開鍵暗号、ならびに秘密鍵 s 、 ymk と平文 s, ym, m とから暗号文 $s, ym, C = smE_{symk}(s, ym, m)$ が作られ、上記秘密鍵 s 、 ymk と暗号文 s, ym, C とから平文 $s, ym, m = smD_{symk}(s, ym, C)$ が作られるような秘密鍵暗号を用いて暗号文を生成する暗号化方法であって、

H および G を関数とし、

暗号化処理として、平文 M と乱数 R 及び r 、公開鍵 p, k を用いて $C_1 = E_{pk}(R, r)$ 、 $C_2 = smE_{symk}(M)$ 及び $C_3 = H(C_1, R, M)$ を生成し $C = (C_1, C_2, C_3)$ を暗号文とすることを特徴とする暗号化方法。

【請求項8】 上記関数 H を任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数 G を k ビットのデータを s ビットに変換するランダム関数とすることを特徴とする請求項7記載の暗号化方法。

【請求項9】 m を平文（暗号の対象となる文書）、 r を乱数、 (p, k, s, k) を公開鍵と秘密鍵の対とすると、 p, k, m, r より暗号文 $C = E_{pk}(m, r)$ が作ら

(3) 001-222218 (P2001-222218A)

れるような公開鍵暗号、ならびに秘密鍵 symK と平文 symM とから暗号文 $\text{symC} = \text{symE}_{\text{symK}}(\text{symM})$ が作られ、上記秘密鍵 symK と暗号文 symC とから平文 $\text{symM} = \text{symD}_{\text{symK}}(\text{symC})$ が作られるような秘密鍵暗号を用いて生成された暗号文であって、

HおよびGを関数とし、

暗号化処理として、平文Mと乱数R及びr、公開鍵pkを用いて $C_1 = E_{pk}(R, r)$ 、 $C_2 = \text{symE}_{g(R)}(M)$ 及び $C_3 = H(C_1, R, M)$ を生成し $C = (C_1, C_2, C_3)$ で表される暗号文を復号する復号方法において、

C及び秘密鍵sk、公開鍵pkより $R' = D_{pk}(C_1)$ 及び $M' = \text{symD}_{g(R')}(C_2)$ を計算し $C_3' = H(C_1, R', M')$ と C_3 とが一致するか否かを検証し、一致すれば、 M' を平文Mとして出力することと特徴とする復号方法。

【請求項10】 上記関数Hを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Gをkビットのデータをsビットに変換するランダム関数とすることを特徴とする請求項9記載の復号方法。

【請求項11】 乱数R、rを発生する乱数発生手順と、

上記乱数R、rと公開鍵pkとを用いて暗号文 $C_1 = E_{pk}(R, r)$ を計算する公開鍵暗号暗号化演算手順と、

上記乱数Rとランダム関数Gとを用いて秘密鍵 $\text{symK} = G(R)$ を計算する第1の関数演算手順と、

上記秘密鍵 symK と平文Mとを用いて暗号文 $C_2 = \text{symE}_{\text{symK}}(M)$ を計算する秘密鍵暗号暗号化演算手順と、

上記乱数Rと上記暗号文 C_1 と上記平文Mと関数Hとを用いて暗号文 $C_3 = H(C_1, R, M)$ を計算する第2の関数演算手順と、

暗号文 $C = (C_1, C_2, C_3)$ を出力する出力手順とを実行するためのプログラムを記憶した記憶媒体。

【請求項12】 乱数R、rと公開鍵pkとを用いて計算された暗号文 $C_1 = E_{pk}(R, r)$ と、上記乱数Rと関数Gとを用いて計算された秘密鍵 $\text{symK} = G(R)$ と平文Mとから計算された暗号文 $C_2 = \text{symE}_{\text{symK}}(M)$ と、上記乱数Rと上記暗号文 C_1 と関数Hとを用いて計算された暗号文 $C_3 = H(C_1, R, M)$ とからなる暗号文 $C = (C_1, C_2, C_3)$ を入力する入力処理と、

上記暗号文 C_1 と秘密鍵skとを用いて乱数 $R' = D_{sk}(C_1)$ を計算する公開鍵暗号復号演算手順と、

上記乱数 R' と上記関数Gとを用いて秘密鍵 $\text{symK}' = G(R')$ を計算する第1の関数演算手順と、

上記秘密鍵 symK' と上記暗号文 C_2 とを用いて平文

$M' = \text{symD}_{\text{symK}'}(C_2)$ を計算する秘密鍵暗号復号演算手順と、

上記平文 M' と上記暗号文 C_1 と上記乱数 R' と関数Hとを用いて暗号文 $C_3' = H(C_1, R', M')$ を計算する第2の関数演算手順と、

上記暗号文 C_3' と上記暗号文 C_3 とを比較する比較手順とを実行するためのプログラムを記憶した記憶媒体。

【請求項13】 上記関数Hを任意のサイズのデータを特定のサイズのデータに変換するランダム関数とし、上記関数Gをkビットのデータをsビットに変換するランダム関数とすることを特徴とする請求項11又は12記載のプログラムを記憶した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、文書を公開鍵暗号を用いた暗号文に変換する暗号化装置、方法、暗号文を解読する復号装置、方法、暗号化装置と復号装置からなる暗号システム、及び暗号化装置、復号装置で用いられるプログラムを記憶した記憶媒体に関するものである。

【0002】

【従来の技術】 一般に、暗号法は共通鍵暗号システムと公開鍵暗号システムの二種類に大別できる。公開鍵暗号システムは、共通鍵暗号システムと問題となる鍵管理の問題や鍵の管理の問題などを解決する方法である。代表的な公開鍵暗号として、RSA暗号、Rabin暗号、ElGamal暗号、楕円曲線暗号（楕円ElGamal暗号）などが挙げられる。

【0003】 これらの公開鍵暗号のうちElGamal暗号、楕円曲線暗号（楕円ElGamal暗号）などは、暗号化処理に乱数が使われ、確率暗号と呼ばれる。

【0004】 暗号文に対する攻撃法には、大きく分けて受動的攻撃と能動的攻撃とがある。受動的攻撃とは、攻撃者が単に暗号文と公開情報から平文を探索することである。能動的攻撃とは、攻撃者は自分が自由に選択した暗号文を正規の受信者に復号してもらうことができる。能動的攻撃に対しても安全な暗号方式を用いることは、より強い安全性を保証する暗号文を構成することを意味する。

【0005】 従来、RSA暗号のような確率的な暗号に基づき、能動的攻撃に強い暗号文を作成する一般的な方法としては、Bellare, RogawayによるOAEP (Optimal Asymmetric Encryption Padding) という方法が知られている (M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption - How to encrypt with RSA" Advances in Cryptology - EUROCRYPT '94, LNCS, Springer-Verlag, 1995)。この方法は、ランダム関数（例えば、SHAなどのハッシュ関数）であり、その具体的な構成法は上記論文に掲載）を2種類用いて構成する方法である。

【0006】

【発明が解決しようとする課題】 しかしながら、上記OA

(4) 001-222218 (P2001-222218A)

EPは確率暗号には適用できないため、確率暗号を用いて能動的攻撃に強い暗号文を作成するための一般的な方法は知られていなかった。

【0007】本発明は、一般的な公開鍵暗号（確率暗号を含む）を用いて能動的攻撃に強い暗号文を作成することができるようにすることを目的としている。

【0008】

【課題を解決するための手段】上記の目的を達成するために、本発明による暗号化装置は、乱数 R 、 r を発生する乱数発生手段（例えば実施の形態における乱数発生器101）と、上記乱数 R 、 r と公開鍵 p 、 k を用いて暗号文 $C_1 = E_{pk}(R, r)$ を計算する公開鍵暗号暗号化演算手段（同公開鍵暗号暗号化演算器103）と、上記乱数 R と関数 G を用いて秘密鍵 $symK = G(R)$ を計算する第1の関数演算手段（同関数演算器G102）と、上記秘密鍵 $symK$ と平文 M を用いて暗号文 $C_2 = symE_{symK}(M)$ を計算する秘密鍵暗号暗号化演算手段（同秘密鍵暗号暗号化演算器104）と、上記乱数 R と上記暗号文 C_1 と上記平文 M と関数 H を用いて暗号文 $C_3 = H(C_1, R, M)$ を計算する第2の関数演算手段（同関数演算器H105）と、暗号文 $C = (C_1, C_2, C_3)$ を出力する出力手段とを設けている。

【0009】本発明による復号装置は、上記暗号化装置で生成された上記暗号文 $C = (C_1, C_2, C_3)$ を入力する入力手段と、上記暗号文 C_1 と秘密鍵 sk を用いて乱数 $R' = D_{sk}(C_1)$ を計算する公開鍵暗号復号演算手段（同公開鍵暗号復号演算器201）と、上記乱数 R' と上記関数 G を用いて秘密鍵 $symK' = G(R')$ を計算する第1の関数演算手段（同関数演算器G202）と、上記秘密鍵 $symK'$ と上記暗号文 C_2 とを用いて平文 $M' = symD_{symK'}(C_2)$ を計算する秘密鍵暗号復号演算手段（同秘密鍵暗号復号演算器203）と、上記平文 M' と上記暗号文 C_1 と乱数 R' と関数 H を用いて暗号文 $C_3' = H(C_1, R', M')$ を計算する第2の関数演算手段（同関数演算器H204）と、上記暗号文 C_3' と暗号文 C_3 とを比較する比較手段（同比較器205）とを設けている。

【0010】本発明による暗号システムは、乱数 R 、 r を発生する乱数発生手段と、上記乱数 R 、 r と公開鍵 p 、 k を用いて暗号文 $C_1 = E_{pk}(R, r)$ を計算する公開鍵暗号暗号化演算手段と、上記乱数 R と関数 G を用いて秘密鍵 $symK = G(R)$ を計算する第1の関数演算手段と、上記秘密鍵 $symK$ と平文 M を用いて暗号文 $C_2 = symE_{symK}(M)$ を計算する秘密鍵暗号暗号化演算手段と、上記乱数 R と上記暗号文 C_1 と上記平文 M と関数 H を用いて暗号文 $C_3 = H(C_1, R, M)$ を計算する第2の関数演算手段と、暗号文 $C = (C_1, C_2, C_3)$ を出力する出力手段とを有する暗号化装置と、上記暗号文 $C = (C_1, C_2, C_3)$ を入力する入力手段と、上記暗号文 C_1 と秘密鍵 sk とを用いて乱数

$R' = D_{sk}(C_1)$ を計算する公開鍵暗号復号演算手段と、上記乱数 R' と上記関数 G を用いて秘密鍵 $symK' = G(R')$ を計算する第3の関数演算手段（同関数演算器G202）と、上記秘密鍵 $symK'$ と上記暗号文 C_2 とを用いて平文 $M' = symD_{symK'}(C_2)$ を計算する秘密鍵暗号復号演算手段と、上記平文 M' と上記暗号文 C_1 と乱数 R' と関数 H とを用いて暗号文 $C_3' = H(C_1, R', M')$ を計算する第4の関数演算手段（同関数演算器H204）と、上記暗号文 C_3' と暗号文 C_3 とを比較する比較手段とを有する復号装置とを備えている。

【0011】本発明による暗号方法は、 m を平文（暗号の対象となる文書）、 r を乱数、 (p, k, sk) を公開鍵と秘密鍵の対とするとき、 p, k, m, r より暗号文 $C_1 = E_{pk}(m, r)$ が作られるような公開鍵暗号、ならびに秘密鍵 $symK$ と平文 $symM$ とから暗号文 $symC = symE_{symK}(symM)$ が作られ、上記秘密鍵 $symK$ と暗号文 $symC$ とから平文 $symM = symD_{symK}(symC)$ が作られるような秘密鍵暗号を用いて暗号文を生成する暗号化方法であって、 H および G を関数とし、暗号化処理として、平文 M と乱数 R 及び r 、公開鍵 p 、 k を用いて $C_1 = E_{pk}(R, r)$ 、 $C_2 = symE_{sk}(M)$ 及び $C_3 = H(C_1, R, M)$ を生成し、 $C = (C_1, C_2, C_3)$ を暗号文とするものである。

【0012】本発明による復号方法は、上記暗号化方法により生成された暗号文を復号する場合に、 C 及び秘密鍵 sk 、公開鍵 p より $R' = D_{pk}(C_1)$ 及び $M' = symD_{sk}(C_2)$ を計算し、 $C_3' = H(C_1, R', M')$ と C_3 とが一致するかどうかを検証し、一致すれば、 M' を平文 M として出力するものである。

【0013】本発明によるプログラムを記憶した記憶媒体は、乱数 R 、 r を発生する乱数発生手段と、上記乱数 R 、 r と公開鍵 p 、 k を用いて暗号文 $C_1 = E_{pk}(R, r)$ を計算する公開鍵暗号暗号化演算手段と、上記乱数 R と関数 G を用いて秘密鍵 $symK = G(R)$ を計算する第1の関数演算手段と、上記秘密鍵 $symK$ と平文 M を用いて暗号文 $C_2 = symE_{symK}(M)$ を計算する秘密鍵暗号暗号化演算手段と、上記暗号文 C_1 と上記平文 M と関数 H を用いて暗号文 $C_3 = H(C_1, R, M)$ を計算する第2の関数演算手段と、暗号文 $C = (C_1, C_2, C_3)$ を出力する出力手段とを実行するためのプログラムを記憶したものである。

【0014】本発明による他のプログラムを記憶した記憶媒体は、上記記憶媒体の処理により生成された上記暗号文 $C = (C_1, C_2, C_3)$ を入力する入力処理と、上記暗号文 C_1 と秘密鍵 sk とを用いて乱数 $R' = D_{sk}(C_1)$ を計算する公開鍵暗号復号化演算手段と、上記乱数 R' と上記関数 G を用いて秘密鍵 $symK' = G(R')$ を計算する第1の関数演算手段と、上記秘密鍵 $symK'$ と上記暗号文 C_2 とを用いて平文 $M' = s$

(15) 001-222218 (P2001-222218A)

ymD_{symk} (C₂) を計算する秘密鍵暗号復号化演算手順と、上記平文M' と上記暗号文C₁ と乱数R' と関数Hとを用いて暗号文C₉' = H(C₁, R', M') を計算する第2の関数演算手順と、上記暗号文C₉' と暗号文C₂ とを比較する比較手段とを実行するためのプログラムを記憶したものである。

【0015】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。本実施の形態は、一般的な公開鍵暗号を用いて能動的攻撃に強い暗号文を構成する方法として、ランダム関数を2回利用するだけで所定の安全性が得られる新しい暗号方式を提案するものである。

【0016】図1は本実施の形態による公開鍵暗号を用いた暗号化装置100を示すブロック図、図2は暗号化装置100で作成された暗号文を解読(復号)する復号装置200を示すブロック図である。上記暗号化装置100及び復号装置200により暗号システムが構成される。

【0017】次に、暗号化処理及び復号処理について説明する。まず、ある公開鍵暗号を仮定する。この公開鍵暗号は、mを平文(暗号の対象となる文書)、rを乱数、(pk, sk)を公開鍵と秘密鍵の対とするとき、暗号文cは、 $c = E_{pk}(m, r)$ で表現する。また、秘密鍵を用いた復号関数は、 D_{sk} で表現する。このとき、mの長さをkビット、rの長さをlビットとする。

【0018】また、ある秘密鍵暗号を仮定する。この秘密鍵暗号では、秘密鍵symkと平文symmから、暗号文symc = $symE_{symk}(symm)$ が作られ、また、秘密鍵symkと暗号文symcから平文symm = $symD_{symk}(symc)$ が復号される。ここで、symkの長さをsビットとする。

【0019】また、Hを任意のサイズのデータを特定のサイズのデータに変換するランダム関数、Gをkビットのデータをsビットに変換するランダム関数とする(このようなランダム関数の具体例については、上記OAPの論文を参照)。

【0020】まず、図1の暗号化装置100による暗号化処理について説明する。図1において、tビットの平文をMとする。乱数発生器101よりkビットの乱数Rとlビットの乱数rを発生させる。そして、関数演算器G102により乱数Rを用いて秘密鍵symk = $G(R)$ を計算する。

【0021】また、公開鍵暗号暗号化演算器103に上記乱数R、rと公開鍵pkとを入力して暗号文C₁ = $E_{pk}(R, r)$ を生成する。次に、秘密鍵暗号暗号化演算器104に、上記Mと関数演算器G102で計算された秘密鍵symkとを入力し、暗号文C₂ = $symE_{symk}(M)$ を生成する。さらに、関数演算器H105に、公開鍵暗号暗号化演算器103で計算された上記暗号文C₁ と乱数Rとを入力して、暗号文C₉' = H(C₁, R,

M) を計算し、C = (C₁, C₂, C₉) を暗号文として出力する。

【0022】次に、図2の復号装置200による復号処理について説明する。図2において、復号装置200には、暗号化装置100で生成された暗号文C = (C₁, C₂, C₉) が入力される。公開鍵暗号復号演算器201は、秘密鍵skとC₁ とから乱数R' = $D_{sk}(C_1)$ を計算する。次に、関数演算器G202により上記R'を用いて秘密鍵symk' = $G(R')$ を計算する。次に、秘密鍵暗号復号演算器203は、上記秘密鍵symk' とC₂ から平文M' = $symD_{symk'}(C_2)$ を計算する。

【0023】次に、関数演算器H204により上記C₁, R', M' より暗号文C₉' = H(C₁, R', M') を計算する。次に、比較器205により、上記C₉' の値と暗号化装置100から入力されたC₉の値とが等しいか否かを検証する。そして、もし等しくなければ、何も出力しない(もしくは、「検証不合格(NG)」を出力する)。もし等しければ(OKなら)、上記M' を元の平文Mとして出力する。

【0024】このように本実施の形態によれば、ランダム関数G、Hを用いることにより、暗号文Cを復号する者は、送信者が暗号文Cの復号結果である平文Mの値を知っていたかどうかを検証できる。従って、復号処理の検証に合格した場合は、送信者が暗号文Cの復号結果である平文Mの値を知っていたことを確認できるため、能動的攻撃に対しても安全性を保証することができる。

【0025】さらに、秘密鍵暗号(symE_{symk}, symD_{symk})及び関数G、Hの演算量が、公開鍵暗号(E_{pk}, D_{pk})の演算量に比べて小さいと仮定すると、本実施の形態による暗号方式の演算量は、元の公開鍵暗号(E_{pk}, D_{pk})の演算量とほぼ同等である。即ち、本実施の形態により処理量のオーバーヘッドをほぼ無くしながら、安全性を向上させることが可能である。

【0026】尚、本実施の形態による暗号化装置100及び復号装置200において、前述した暗号化処理及び復号処理をそれぞれコンピュータシステムで実行する場合、そのコンピュータシステムにおけるCPUが実行するプログラムを記憶した記憶装置は、本発明によるプログラムを記憶した記憶媒体を構成する。この記憶媒体としては、各種のディスク媒体や半導体メモリ、磁気記録媒体等を用いることができる。

【0027】

【発明の効果】以上説明したように本発明によれば、暗号文に対する能動的な攻撃に対して高い安全性を保証することができ、かつ少ない演算量で高い安全性を保証することができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態による暗号化装置100の構成を示すブロック図である。

I(6) 001-222218 (P2001-222218A)

【図2】 本発明の実施の形態による復号装置200の構成を示すブロック図である。

【符号の説明】

100 暗号化装置

101 乱数発生器

102 関数演算器G

103 公開鍵暗号暗号化演算器

104 秘密鍵暗号暗号化演算器

105 関数演算器H

R, r 乱数

symk 秘密鍵

C₁, C₂, C₃ 暗号文

M 平文

200 復号装置

201 公開鍵暗号復号演算器

202 関数演算器G

203 秘密鍵暗号復号演算器

204 関数演算器H

205 比較器

sk 秘密鍵

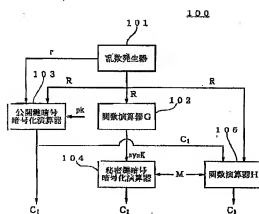
R' 乱数

symk' 秘密鍵

C₃' 暗号文

M' 平文

【図1】



【図2】

